ANNEX B (INTELLIGENCE) to TRADOC Mobilization and Operations Planning and Execution System 1-97 (TMOPES 1-97)

1. SITUATION.

a. Strategic Threat. See Appendix 1.

b. CONUS Threat. See Appendix 2.

c. Assumptions. See basic plan.

2. MISSION: On order, Deputy Chief of Staff for Intelligence (DCSINT), provides the TRADOC leadership the intelligence and security support to implement TRADOC support of approved operations, contingencies, and any level of mobilization.

3. EXECUTION.

a. Concept of Operations.

(1) Planning for the performance of intelligence, counterintelligence (CI) and security functions is accomplished as an integral part of overall command planning.

(2) Define intelligence objectives in terms of Priority Intelligence Requirements (PIR) based on TRADOC Commander's guidance and intelligence support requirements.

(3) To satisfy intelligence, CI and security support requirements during full mobilization, DCSINT forms an Intelligence Support Cell (ISC) from existing personnel resources. During lesser levels of mobilization or operational support, DCSINT provides required intelligence and security support in accordance with current guidance from the TRADOC Chief of Staff and Command Group.

(4) Priority Intelligence Requirements (PIR). See Appendix 3 this ANNEX.

b. Tasks.

(1) DCSINT. (During full mobilization, otherwise as indicated in para 3.a.(3) above.)

(a) Establish and maintain coordination with other MACOMs, DA DCSINT, 902d Military Intelligence Group, and National Intelligence Agencies.

(b) Ensure timely, accurate intelligence, counter-intelligence and security, and weather support is provided to the TRADOC Commander, staff, and subordinate commanders.

(c) Establish and maintain an intelligence/terrorist threat Order of Battle and country file data base to support intelligence requirements.

(d) Maintain liaison with local, state, and federal law enforcement agencies.

(e) Prepare intelligence reports/summaries and briefings for the TRADOC Command Group and staff.

(f) Provide information, automation, communication, and personnel security program support to ensure protection of sensitive and classified information.

(2) Counterintelligence. See Appendix 4 this ANNEX.

(3) Meteorology. See Appendix 5 this ANNEX.

(4) Special Security Office (SSO) Support. Submits compelling need requests for Sensitive Compartmented Information (SCI) access, approves SCI billets, indoctrinates for SCI, and establishes both Field Sensitive Compartmented Information Facilities (SCIFs) and Temporary Secure Working Areas. Provides communications support via the Defense Special Security Communications Support (DSSCS) system at mobilization sites. Provides access to available intelligence data bases.

(5) Mapping, Charting, and Geodesy (MC&G).

(a) DCSINT assists in map procurement, production and distribution. The provisions of TRADOC Pamphlet 420-4 describe appropriate procedures.

(b) Under emergency conditions, use local and regional map repositories or reprinted maps.

c. Coordinating Instructions. The DCSINT Intelligence Support Cell (ISC) prepares the following reports:

(1) The Daily Intelligence Summary (DISUM) containing a synopsis of major events in selected world regions, threats against TRADOC and descriptions of incidents affecting security.

(2) Threat advisories from HQ TRADOC or TRADOC installations to higher headquarters, or DCSINT, to advise of threats, impending threats, potential threats, disruptions and actions taken.

(3) Situation Reports (SITREPs) as directed.

(4) Daily Staff Reports to record daily events.

4. ADMINISTRATION AND LOGISTICS. See basic plan.

5. COMMAND AND CONTROL. Upon execution of TMOPES, Intelligence and Security functions remain under the operational control of the DCSINT as indicated in para 3.a.(3) above.

HARTZOG
GEN

OFFICIAL:

O'DAWE
Deputy Chief of Staff
for Intelligence

APPENDIXES:
1 - Strategic Threat
2 - CONUS Threat
3 - Priority Intelligence Requirements
4 - Counterintelligence
5 - Meteorology

Appendix 1 (Strategic Threat) to ANNEX B (INTELLIGENCE) to TMOPES 1-97

1. Overview. The disintegration of the Soviet Union has allowed ethnic and other conflicts to reemerge in Eastern Europe, the Caucasus, and Central Asia. The potential for conflict in the Middle East and South Asia, where many states import arms and seek to develop weapons of mass destruction, remains high. Communist regimes remain in place in China, Cuba, and North Korea. The foundations for political systems in Sub-Saharan Africa and Latin America are fragile and could be undermined by regional conflict and economic turmoil. Finally, the proliferation of nuclear, chemical, biological, and advanced technological weaponry continues to be of grave concern.

2. Russia and other Successor States to the USSR. The disintegration of the former Soviet Union and the severe economic dislocation caused by the transition from communism to capitalism has greatly reduced, for the near term, the potential for Russian military aggression against the U.S. and its NATO allies. Russia's conventional military capabilities continue to suffer, as evidenced by the poor showing in Chechenya and incidents of starvation at remote bases. Nevertheless, Russia still possesses a formidable strategic nuclear arsenal with the capability to threaten the U.S. The other successor states to the Soviet Union pose little or no direct threat to the U.S. Belarus, Kazakhstan, and Ukraine are in the process or have completed transferring their nuclear weapons to Russia. However, the danger remains that, due to economic necessity, some of the successor states will sell advanced weapons or technology inherited from the USSR to rogue states such as Libya, Iran, or Iraq. Also, conflicts in the Caucasus and Central Asia have the potential to spill over into the Middle East.

3. Eastern Europe. The Eastern European countries continue to shift their military establishments from postures dictated by defunct Warsaw Pact requirements to smaller forces reconfigured and deployed to meet purely national needs. Most governments in the region are making steady progress in establishing Western-style civilian-controlled defense forces and are seeking membership in NATO. Despite these positive trends, the threat remains of armed conflicts arising from historical or ethnic grievances, such as the case in the former Yugoslavia.

4. Middle East. In the Middle East, lasting regional stability remains elusive. Over the next 10 to 15 years, Iran and Iraq will continue their competition for hegemony in the Persian Gulf and will seek to strengthen their military capabilities. Another war between these two states is possible. Libya continues its attempts to produce chemical weapons. Over the next ten years, several Middle Eastern states will acquire medium range ballistic

missiles, which will extend a threat of attack (possibly nuclear) to parts of Europe and Eurasia. Despite Israel's peace agreements with Egypt, Jordan, and the Palestinians, renewed Arab-Israeli conflict is possible due to Syrian claims to the Golan Heights and the continued presence of radical Muslim militia groups in Lebanon.

5. South Asia. Tensions between India and Pakistan remain serious. They both maintain large military establishments, and if hostilities break out between the two, nuclear weapons could be employed by either country. Compounding the problem, both may deploy short-range ballistic missiles by the end of the decade.

6. East Asia. The situation on the Korean Peninsula poses the most serious short term security problem the U.S. faces in East Asia. North Korea maintains the option to unify the Peninsula by force. Throughout the decade, the quantitative military balance will continue to favor the North. Despite continuing efforts in the near term, the South will not achieve an independent capability to defend itself, and it will remain dependent on U.S. support. The status of North Korea's nuclear weapons program remains a cause for concern. North Korea could have a nuclear weapon within two to three years of a resumption of the program. China poses the greatest long term threat to U.S. interests in East Asia. The Chinese have become increasingly aggressive in asserting their claims to Taiwan and the entire South China Sea. They are purchasing significant amounts of advanced conventional weapons (including SU-27 aircraft) at bargain prices from the cash-strapped Russians. China is reportedly also seeking to buy SS-18 ICBMs from Russia, ostensibly for its space program, which would provide the capability to launch a nuclear strike on CONUS. Chinese sales of ballistic missiles and nuclear technology, particularly to rogue regimes, pose a direct threat to U.S. interests.

7. Sub-Saharan Africa. Sub-Saharan Africa is perhaps the most unstable region in the third world, and will continue to be so over the next decade. U.S. forces will face continued involvement in humanitarian relief operations or evacuations of U.S. citizens, such as those in Somalia, Rwanda, Zaire, and Liberia.

8. Latin America. The continued strength of democratic governments, the weakening of some insurgencies, and the end of Soviet influence are positive developments. However, narcotics trafficking, sometimes associated with insurgent groups, threatens several Latin American countries. Cuba remains a concern, due to the continued presence of a Russian SIGINT base

and the economic instability caused by the loss of Russian military aid.

9. Weapons and Technology Proliferation. The proliferation of nuclear, chemical, biological, and advanced conventional weapons technology is of critical concern. Many third world countries are developing dual-use technologies that could be diverted for the production of such weapons. This situation is exacerbated by the proliferation of conventional weaponry of ever-increasing sophistication to some of the most unstable parts of the world, causing a potential threat to U.S. forces or allies.

10. Another emerging threat is information warfare. Adversaries are aware of U.S. dependency on information systems. They will attempt to exploit U.S. dependency across the information warfare spectrum by the introduction of viruses, manipulation of and illegal access to databases, and ultimately, the destruction of information system and equipment.

Appendix 2 (CONUS Threat) to ANNEX B (INTELLIGENCE) to TMOPES 1-97

1. Overview. TRADOC's mission and location combine to make it a valuable target for a terrorist attack. In recent years, both foreign Muslim terrorists and domestic anti-government groups have demonstrated the ease with which they can cause major damage and loss of life in the U.S. Individual alertness, training, and preparation for possible terrorist acts have proven to be effective deterrents. Every individual must be familiar with the threat of terrorism, how terrorists operate, and the procedures that are effective in minimizing the threat. TRADOC must continually be aware of the terrorist threat probabilities and train the force regarding proper safety measures.

2. Foreign Intelligence Service Threat. The demise of the Soviet Union and Warsaw Pact have changed, but not eliminated, the espionage threat. Foreign intelligence services (including those of some U.S. allies) now place a higher priority on collection of U.S. scientific and technical information. Through increased emphasis on security procedures (particularly in regard to communications and computers) and strict adherence to U.S. Army protection programs, TRADOC personnel can reduce the flow of sensitive U.S. technology to foreign adversaries/competitors.

3. Threat Data. Local and national level counterintelligence agencies are responsible for collecting and disseminating terrorist threat data. Upon mobilization alert, CONUS threat information is made available for further distribution to appropriate personnel.

4. Early Warning. Military activities are especially vulnerable during the early stages of mobilization. Early warning and security awareness measures are implemented.

Appendix 3 (Priority Intelligence Requirements) to Annex B (INTELLIGENCE) to TMOPES 1-97

1. Information on the following special areas of interest is required to fulfill TRADOC PIR.

a. What are the military capabilities of potential threat nations? Include equipment, doctrine, tactics, strength figures, organization and training, force composition and disposition, aims and objectives of enemy forces.

b. Which emerging technologies or weapons systems have proliferated to the extent that they threaten U.S. ground forces?

c. What nation’s organizations possess or are pursuing the development and/or acquisition of nuclear, chemical or biological agents and delivery means to include tactical ballistic missiles?

d. What are potential enemy countries' or organizations' capabilities to employ terrorism, Special Operations Forces, agents or sabotage groups to hinder U.S. mobilization capabilities and deployment?

e. What TRADOC installations/activities would be potential targets of enemy forces or long range attack means such as missile strikes? What would be the effects of such attacks?

f. How, when, and by whom will our digital information systems and global command and control systems be attacked?

g. What is the threat to TRADOC installations from domestic or international terrorist groups/organizations?

Appendix 4 (Counterintelligence) to Annex B (INTELLIGENCE) to TMOPES 1-97

1. SITUATION.

a. Enemy Forces. (See Appendix 1 and 2)

b. Friendly Forces. (See basic plan)

c. Assumptions. During periods of operational or contingency support, foreign intelligence services increase their efforts to obtain data pertaining to TRADOC mobilization, training, doctrine, or combat developments.

2. MISSION. On order, the DCSINT’s Director of Security provides security support to successfully complete military operations.

3. EXECUTION.

a. Concept of Operations. TRADOC expands its counterintelligence (CI) and security program to protect classified and sensitive unclassified information.

b. Tasks. During operations, contingencies, and/or any level of mobilization, the Director of Security and TRADOC installation and activity security managers perform the following:

(1) Counterintelligence:

(a) Assess foreign intelligence service capabilities to impede mobilization efforts.

(b) Receive, analyze, and disseminate information and intelligence that may impact mobilization missions.

(c) Maintain liaison with local and national CI elements to ensure a continuous channel of communication.

(d) Provide CI for TRADOC's operations security (OPSEC) initiatives.

(e) Participate in OPSEC surveys to identify and protect all sources of exploitable information, communications, and other electronic weaknesses.

(f) Monitor Sabotage and Espionage Directed Against the Army (SAEDA) programs, particularly with respect to identification of incidents and reporting requirements.

(2) Information Security:

(a) Expand oversight and security awareness programs to ensure sensitive material is safeguarded and disseminated on a strict need-to-know basis.

(b) Ensure the timely distribution of all pertinent and newly developed security classification guidance.

(c) Oversee security compromise investigations and ensure command corrective action is prompt and appropriate.

(d) Advise mobilization units to review classified documents prior to arrival at mobilization stations to ensure only operational essential classified material is retained.

(3) Information Systems Security (ISS):

(a) The TRADOC Information Systems Security Program Manager (ISSPM), assigned to the Directorate of Security, DCSINT, provides ISS guidance and policy for all of TRADOC. ISS Managers (ISSM), assigned to each installation or region, conduct risk analyses to determine how to counter threats to systems at mobilization sites. The Information Systems Security Officers (ISSO), assigned to HQs or Center and School directorates and offices, coordinate formal accreditation upon completion of risk analyses. Tactical and mobile Automated Information Systems (AIS) must receive the level of security consistent with the threat situation.

(b) The ISSO notifies the Information Systems Security Manager (ISSM) when a change in the sensitivity designation is deemed necessary for any automated system within his purview and take appropriate action based upon such change. This requirement is particularly critical at data processing activities which have been or could be designated as relocation sites for another automated system of higher sensitivity.

(c) ISSOs must consider control of compromising emanations protection requirements for computers processing classified data under provisions of AR 380-19-1.

(d) Each ISSO is responsible for the day-to-day security of AIS facilities, equipment, and expendable media belonging to or in the custody of the staff or office.

(e) ISSOs make sure all AIS media, as defined in AR 380-19, are treated, handled, and destroyed as "CONTROLLED UNCLASSIFIED INFORMATION" (CUI) or “SENSITIVE BUT UNCLASSIFIED” (SBU) as a minimum, and marked accordingly.

(f) ISSOs develop procedures for routine and emergency purging of internal memory and AIS media in the event of civil disturbances.

(g) ISSOs make sure computer operators and maintenance personnel are cleared to the level of sensitivity of information processed.

(h) ISSOs ensure that users do not place classified or sensitive information on unsecure e-mail systems or internet home-pages.

(4) Personnel Security: Upon declaration of Presidential Selected Reserve Call-up (PSRC), TRADOC requests authority from HQDA, DCSINT (DAMI-CIS) to waive investigative requirements contained in AR 380-67 and issue interim security clearances as operationally necessary without prior approval of the U.S. Army Central Personnel Security Clearance Facility.

(5) Communications Security:

(a) One of our greatest vulnerabilities is our telephone system (to include cellular phones), therefore, make every effort to use secure phones and do not “talk around” classified or disclose sensitive information during non-secure telephone calls.

(b) Headquarters conducting classified and sensitive operations should consider whether they need Communications Security (COMSEC) monitoring support.

(c) Units take every precaution to ensure the security of keying material, including 24-hour armed guards where required.

(d) TRADOC expeditiously disseminates any changes in DA and command policy for security of crypto material and/or controlled cryptographic items.

(6) Information Disclosure: Ensure all information for release to foreign representatives are reviewed and approved by appropriate security personnel prior to releasing information to the requester.

4. ADMINISTRATION AND LOGISTICS. (See basic plan)

5. COMMAND AND CONTROL. During both full mobilization and periods other than full mobilization, Security Directorate remains part of the DCSINT.

Appendix 5 (Meteorological) to Annex B (INTELLIGENCE) to TMOPES 1-97

REFERENCES.

AR 115-12, "U.S. Army Requirements for Weather and Climatological Support".
AR 115-10/AFJI 15-157, "Meteorological Support for the U.S. Army".

1. GENERAL. The U.S. Air Force (USAF) provides meteorological support for the U.S. Army through the Directorate of Weather (DOW) at Air Force Major Commands and functionally aligned Air Support Operations Groups (ASOGs).

2. CONCEPT OF SUPPORT.

a. The USAF Staff Weather Officer (SWO) assigned to TRADOC DCSINT provides meteorological support for TRADOC. The SWO coordinates directly with the TRADOC Commander and staff concerning weather support. SWOs assigned to the Intelligence Center and Combined Arms Center are responsible for weather support at those locations.

b. The 3rd Air Support Operations Group, Fort Hood, TX and the 18th Air Support Operations Group, Fort Bragg, NC operate fixed weather stations to provide weather support to selected TRADOC installations IAW AR 115-12.

3. COMMUNICATIONS AND LOGISTICS. Joint Army and Air Force responsibilities for fixed and mobile weather communications and logistic support are specified in AR 115-10/AFJI 15-157. Specific communications and/or logistics requirements for the contingency are addressed in operations plans.

4. OPERATIONS PLANS. Operations plans include a weather annex or appendix specifying meteorological support required, how data is provided and the level of support by Air Force weather units IAW AR 115-12. Operations plans will include the level support the Army customer provides the assigned weather unit IAW AR 115-12 and AR 115-10/AFJI 15-157. Climatological data, as well as, solar and lunar tables are provided, as required.